Bloomberg Tax

Tax Management Memorandum™

January 30, 2025

Puerto Rico Health and Welfare Plan Sponsors Need Cybersecurity

By Carlos Gonzalez
BenefitsPuertoRico.com

Puerto Rico benefits and compensation attorney Carlos Gonzalez shares his practical experience with, and recommendations on, the evaluation of the cybersecurity measures of insurance companies servicing healthcare and welfare benefit plans operating in Puerto Rico.

ERISA-covered health and welfare plans operating in Puerto Rico must not only follow certain cybersecurity rules themselves but should also implement specific procedures in order to evaluate the cybersecurity measures of service providers to their plans operating on the Island. The following are observations and recommendations on the relevant rules, and the process that companies doing business in Puerto Rico should follow for evaluating the cybersecurity measures of the service providers of their plans operating on the Island.

Background

In its April 14, 2021, cybersecurity guidance, the Employee Benefits Security Administration of the US Department of Labor reminded sponsors of ERISA-covered plans of their fiduciary duty to take appropriate measures for identifying and mitigating the cybersecurity risks associated with the establishment and operation of their retirement plans. Among other things, this guidance requires plan sponsors and other fiduciaries to prudently select service providers with strong cybersecurity practices and periodically monitor their activities. For a summary of the main aspects to be considered when evaluating the cybersecurity measures of service providers to retirement plans in operation in Puerto Rico, readers should refer to *Cut Cyber Breaches, Service Fees for Puerto Rico Benefit Plans* (July 31, 2024).

On September 6, 2024, EBSA issued Compliance Assistance Release No. 24-1855-NAT to indicate that its cybersecurity guidance of April 14, 2021, is intended to apply to all employee benefits plans covered by ERISA, including health and welfare benefit plans.Thus, plan sponsors should also evaluate the cybersecurity measures of the service providers to such plans.

Health Plans Recommendations

ERISA, HIPAA, and the HITECH Act apply in Puerto Rico just as they do in the US (*see* ERISA §3(10); 42 U.S.C. §1395x(x) and §410(h); 45 C.F.R. §160.103; 42 U.S.C. §300jj(15)). Therefore, covered entities and their business associates servicing health plans in Puerto Rico have the same obligations that apply in the US to safeguard the privacy and security of the protected health information (PHI) they create, maintain, receive, or transmit in connection with, or as a result of, their services to the plans.

For example, covered entities and business associates are required to implement administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic PHI; protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI; and guard against any reasonably anticipated uses or disclosures of electronic PHI not otherwise required or allowed under the HIPAA privacy rule (45 C.F.R. §164.306(a)). Prior to sharing electronic PHI with a business associate, a covered entity must enter into a contractual agreement with the business associate whereby the latter commits to fully comply with the HIPAA privacy and security rules (45 C.F.R. §504(e)).

*Carlos Gonzalez is President of BenefitsPuertoRico.com, a law firm assisting US and international companies with Puerto Rico operations with employee benefits and executive compensation matters, and is the author of Tax Management Portfolio 324-2nd T.M., *International Pension Planning — Puerto Rico.* The author would like to thank Microsoft's in-house ERISA counsel, Garrett Fenton, for his assistance with the preparation of this article.

Whenever business associates discover that unsecured PHI has been impermissibly accessed, used, or disclosed, they must notify the covered entity.And covered entities must give notification of PHI breaches to both affected individuals and the Department of Health and Human Services (HHS) (45 C.F.R. §164.400).For more information about the HIPAA privacy and security rules in general, readers should refer to 389 T.M., *Medical Plans—COBRA, HIPAA, HRAs, HSAs and Disability*.

Fully Insured Health Plans and HMOs. In the case of fully insured health plans and HMOs, which, given their small size, comprise the vast majority of the health plans in operation in Puerto Rico, the covered entity subject to HIPAA is the insurance company that issues and handles benefit claims under the underlying insurance contract, not the employer that establishes or sponsors the plan (45 C.F.R. §160.103). For more information about the type of health plans regularly used in Puerto Rico, readers should refer to *How U.S. Employers Provide Health Plans to Puerto Rico Employees* (64 Tax Mngmt. Memo. 17 (Aug. 14, 2023)).

Puerto Rico Rules. The HIPAA privacy and security rules do not preempt state laws relating to the privacy of individually identifiable health information that are more stringent than HIPAA, or that HHS determines are necessary to prevent fraud or abuse in the provision or payment of health care services or to ensure appropriate state regulation of insurance and health plans (45 C.F.R. §160.203). Currently, Puerto Rico does not have such non-preempted state laws. While Chapter 14 of the Puerto Rico Health Insurance Code (PRHIC) imposes on insurance companies – not on employers – various requirements for the protection of PHI privacy, the local rules are modeled after and intended to operate like the equivalent HIPAA privacy rules, and in the event of conflict between the local rules and the HIPAA rules, the latter always prevail (PRHIC Article 14.020, 26 L.P.R.A. §9232). As for PHI security, the PRHIC simply adopts by reference the equivalent HIPAA rules (Article 14.050A, 26 L.P.R.A. §92A).Therefore, compliance with the HIPAA privacy and security rules automatically results in compliance with the Puerto Rico privacy and security rules.

Plan Sponsors. In light of this regulatory framework, companies that sponsor health plans operating in Puerto Rico generally are limiting their cybersecurity evaluation process to obtaining from the insurance company that insures and administers the plan:

1. written confirmation that, in administering the plan, the insurance company is complying with the relevant HIPAA privacy and security rules (e.g., it has in place and properly follows a HIPAA compliance policy and obtained the necessary business associate agreements),
2. a copy of the most recent version of the HIPAA compliance policy,
3. a copy of the most recent independent cybersecurity audit report (e.g., SOC (Service Organization Control) 2 Type II report (audit on how a cloud-based service provider handles sensitive information over a period of time)), and
4. evidence of the insurance company's cybersecurity liability insurance policy (e.g., a copy of the declarations page).

Ideally, insurance companies would also provide sponsors with a summary or track record of their cybersecurity incidents, but in practice they are not doing so. And since Puerto Rico health plans generally are fairly small, plan sponsors do not have much financial leverage for forcing insurance companies to change their position.

Some companies are going a step further and, unless this is already covered by the underlying insurance policy or services agreement, are requesting from the insurance company written confirmation that:

1. they will notify the plan sponsor of subsequent changes to the HIPAA compliance policy, audit report, and cybersecurity insurance policy (i.e., establish ongoing notification obligation),
2. they will notify the plan sponsor promptly upon detecting a cybersecurity breach or incident and will implement proper mitigation measures, and
3. absent a plan participant's prior written authorization, they will not use the participant's private or confidential information for sales and marketing purposes.

In the author's opinion, plan sponsors are not required to audit or independently validate the insurance company's written assurances and related documents. HIPAA privacy and security rules have been in place for over twenty years; and by now, all healthcare insurance companies operating in Puerto Rico are thoroughly familiar with them, so this recent cybersecurity evaluation requirement should not be viewed as an obligation to educate or question insurance companies on their HIPAA compliance duties.

ISSN 0148-8295

Other Welfare Plans Recommendations

Rule No. 108. Like health plans, most other employee welfare benefit plans operating in Puerto Rico are fully insured.Therefore, through ERISA's §514(b)(2) "savers clause," they are subject to local insurance laws and regulations.For health plans, that essentially means complying with the PRHIC, which, as far as privacy and security are concerned, boils down to complying with HIPAA. Since HIPAA does not apply to non-healthcare welfare plans (45 C.F.R. §160.102(a)(1) and §160.103), the question becomes, what sort of cybersecurity rules apply to other welfare plans in Puerto Rico? Effective September 9, 2024, the answer is Rule No. 108 of Puerto Rico's Regulations of the Insurance Code, *Cybersecurity Standards for the Insurance Industry* (Rule No. 108).

Modeled after the *Insurance Data Security Model Law* issued by the National Association of Insurance Commissioners (NAIC Model Law) , Rule No. 108 requires all insurance companies doing business in Puerto Rico to develop, implement, and periodically update a cybersecurity program reasonably designed to protect the confidentiality, integrity, and availability of the nonpublic information kept in their computer, communications, or information systems and ensure the security of such systems. For these purposes, "nonpublic information" basically means:

- the personal identifiers of plan participants and beneficiaries living in Puerto Rico (e.g., name, address, Social Security number, driver's license, bank or credit card number, and other personal financial information), and
- their biometric records (e.g., information on the past, present, or future history, treatment, or payment for an individual's health conditions).

Rule No. 108 does not regulate nor impose any requirements on employers doing business in Puerto Rico, their ERISA plan administrative committees, or self-funded employee benefits plans.

Cybersecurity Program. Among other things, the cybersecurity program should establish:

- strong controls for accessing customer accounts and information systems, such as multi-factor authentication security methods;
- regular risk assessment, testing, and monitoring requirements;
- backup systems for retrieving information in the event of technological failures, business emergencies, or environmental hazards;
- encryption protections for data transmitted or stored electronically;
- protocols for the management, retention, and periodic destruction of confidential information;
- incident response plans (i.e., the process to be followed and mitigation measures to be implemented upon a cybersecurity incident);
- regular employee trainings on cybersecurity matters; and
- board of directors and executive-level program oversight.

By June 30th of each year, the insurance company must submit with the Office of the Puerto Rico Insurance Commissioner (commonly known by its Spanish initials as "OCS") a written statement certifying that it is complying with the cybersecurity program mandates of Rule No. 108 (§8).

If, as is oftentimes the case, the insurance company transfers nonpublic information to third party vendors or independent contractors, the insurance company must perform a due diligence evaluation of their cybersecurity systems before engaging them and confirm that they have established and implemented their own cybersecurity program before transferring or sharing any nonpublic information with them.

If the insurance company learns that a cybersecurity incident has occurred or may have occurred, it must investigate the matter as soon as possible and prepare a written report thereof. At a minimum, the report must address whether the cybersecurity incident actually occurred; the scope and nature of the incident; the nonpublic information affected by it; and the measures to be implemented to restore the security of affected nonpublic information and prevent similar incidents in the future. Upon request, the insurance company must share this report with OCS (Rule No. 108, §9).

If the insurance company determines that the cybersecurity incident actually breached the security of nonpublic information of individuals residing in Puerto Rico, it must send a written notice of the incident to the affected individuals within ten days of concluding its investigation. And, if the incident involved more than 250 local residents, it must also notify OCS within 72 hours of concluding the investigation (Rule No. 108, §10).

Just as with health plans, rather than auditing or independently evaluating the cybersecurity measures of

ISSN 0148-8295

insurance companies for welfare plans in Puerto Rico, employers should limit their cybersecurity evaluation process to obtaining from the corresponding insurance company:

- written confirmation that, in administering the plan, the insurance company is complying with Rule No. 108;
- a copy of the most recent annual compliance certification to OCS and, if possible, the cybersecurity policy itself;
- a copy of the most recent independent cybersecurity audit report (e.g., SOC 2 Type II report), if any, and
- evidence of the insurance company's cybersecurity liability insurance policy (e.g., a copy of the declarations page).

Risk-adverse employers might also consider requesting the insurance company to provide written confirmation that:

- it will notify the plan sponsor of subsequent changes to the cybersecurity policy, audit report, and insurance policy,
- it will notify the plan sponsor promptly upon detecting a cybersecurity breach or incident and will implement proper mitigation measures (e.g., notify the employer whenever an incident requiring notification to OCS or affected individuals under Rule No. 108, §9, occurs), and
- absent a plan participant's prior written authorization, it will not use the participant's private or confidential information for sales and marketing purposes.

It is doubtful that insurance companies will agree to provide employers with a copy of their cybersecurity incident reports.

Following US Process in Puerto Rico. Finally, since Rule No. 108 is modeled after the NAIC Model Law and about half the states have already implemented their own versions of the NAIC Model Law within their insurance laws or regulations, the same ERISA-compliant cybersecurity evaluation process followed by employers in the states that have adopted the NAIC Model Law, or a reasonable facsimile thereof, should suffice in Puerto Rico. No need to reinvent the wheel when the underlying rules are pretty much the same.

This article does not necessarily reflect the opinion of Bloomberg Industry Group, Inc., the publisher of Bloomberg Law and Bloomberg Tax, or its owners.

ISSN 0148-8295